IN THE CLAIMS

11

ı

Please amend the claims as follows:

- --1. (Amended) A method in a data processing system for maintaining multiple secure user private keys in a non-secure storage device, said method comprising the steps of:
- establishing a master key pair for said system, said master key pair including a master private key and a master public key;
 - storing said master key pair in a protected storage device;
- establishing a unique user key pair for each of multiple users, each of said user key pairs including a user private key and a user public key;

encrypting each of said user private keys utilizing said master public key; and

storing each of said encrypted user private keys in said non-secure storage device, wherein each of said encrypted user private keys is secure while stored in said non-secure storage device.--

- 2. (Unchanged) The method according to claim 1, further comprising the steps of:
- establishing an encryption device having an encryption engine and said protected storage device; and
- said protected storage device being accessible only through said encryption engine.

- --3. (Amended) The method according to claim 2, further comprising the step of said encryption engine encrypting each of said user private keys utilizing said master public key stored in said 2 protected storage device .--3 --4. (Amended) The method according to claim 3, further comprising the steps of: an application generating a message to transmit to a recipient; 2 said encryption engine decrypting a particular user's private key utilizing said master private key; said encryption engine encrypting said message utilizing said decrypted particular user's private key and said recipient's public key; and said system transmitting said encrypted message to said recipient.--7 --5. (Amended) The method according to claim 4, wherein the step of establishing a unique user key pair for each of multiple users further comprises the step of associating each said user key 2 pair with an application .--3
 - --6. (Amended) The method according to claim 5, further comprising the steps of:
- establishing a certificate, said certificate being associated with said application, said particular user's private key, and said particular user;

said encryption engine decrypting said particular user's private key; and said encryption engine utilizing said decrypted particular user's private key messages transmitted by said application7. (Amended) The method according to claim 1, wherein said step of storing ea encrypted user private keys in said non-secure storage further comprises the step of said encrypted user private keys in a hard drive8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system9. (Amended) A data processing system for maintaining multiple secure user pr	ilizing said
said encryption engine decrypting said particular user's private key; and said encryption engine utilizing said decrypted particular user's private key messages transmitted by said application7. (Amended) The method according to claim 1, wherein said step of storing ea encrypted user private keys in said non-secure storage further comprises the step of said encrypted user private keys in a hard drive8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system9. (Amended) A data processing system for maintaining multiple secure user pr	within said
said encryption engine utilizing said decrypted particular user's private key messages transmitted by said application 7. (Amended) The method according to claim 1, wherein said step of storing ea encrypted user private keys in said non-secure storage further comprises the step of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user pro-	d certificate;
said encryption engine utilizing said decrypted particular user's private key messages transmitted by said application 7. (Amended) The method according to claim 1, wherein said step of storing ea encrypted user private keys in said non-secure storage further comprises the step of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user pro-	
7. (Amended) The method according to claim 1, wherein said step of storing ear encrypted user private keys in said non-secure storage further comprises the step of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user pro-	
7. (Amended) The method according to claim 1, wherein said step of storing ear encrypted user private keys in said non-secure storage further comprises the step of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user pro-	
7. (Amended) The method according to claim 1, wherein said step of storing ear encrypted user private keys in said non-secure storage further comprises the step of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user pro-	y to encrypt
encrypted user private keys in said non-secure storage further comprises the step of of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of a unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user processing system for maintaining multiple secure user processing system for maintaining multiple secure user processing system.	
encrypted user private keys in said non-secure storage further comprises the step of of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of a unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user processing system for maintaining multiple secure user processing system for maintaining multiple secure user processing system.	
of said encrypted user private keys in a hard drive 8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user processing syst	ch of said
8. (Amended) The method according to claim 7, further comprising the step of unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system9. (Amended) A data processing system for maintaining multiple secure user processing system	of storing each
unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user processing system.	
unique user key pairs being capable of being utilized only in said data processing a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user processing system.	
a particular user key pair is established, wherein said particular user key pair is no being utilized in a second data processing system 9. (Amended) A data processing system for maintaining multiple secure user processing system.	
being utilized in a second data processing system9. (Amended) A data processing system for maintaining multiple secure user pr	system wherein
9. (Amended) A data processing system for maintaining multiple secure user pr	t capable of
non-secure storage device, comprising:	ivate keys in a
an encryption device included within said system for establishing a master	
said system, said master key pair including a master private key and a master publ	ic key;

Docket No. RP9-98-089 5

a protected storage device for storing said master key pair;

5

6	said encryption device executing code for establishing a unique user key pair for each of
7	multiple users, each of said user key pairs including a user private key and a user public key;
8	said encryption device executing code for encrypting each of said user private keys
9	utilizing said master public key; and
10	a non-secure storage device for storing each of said encrypted user private keys, wherein
11	each of said encrypted user private keys is secure while stored in said non-secure storage device
12	-
.1	10. (Unchanged) The system according to claim 9, further comprising:
2	said encryption device including an encryption engine and said protected storage device;
3	and
4	said protected storage device capable of being accessed only through said encryption
5	engine.
i	11. (Amended) The system according to claim 10, further comprising said encryption engine
2	executing code for encrypting each of said user private keys utilizing said master public key
3	stored in said protected storage device
1	12. (Amended) The system according to claim 11, further comprising:
2	an application capable of generating a message to transmit to a recipient:

3	said encryption engine executing code for decrypting a particular user's private key
4	utilizing said master private key;
5	said encryption engine executing code for encrypting said message utilizing said
6	decrypted particular user's private key and said recipient's public key; and
7	said system transmitting said encrypted message to said recipient
1	13. (Amended) The system according to claim 12, further comprising said system executing
. 2	code for associating each said user key pair with an application
1 7	14. (Amended) The system according to claim 13, further comprising:
)	said system executing code for establishing a certificate, said certificate being associated
3	with said application, said particular user's private key, and said particular user;
4	in response to said particular user attempting to access said application utilizing said
5	certificate, said encryption engine executing code utilizing said certificate for determining a
6	location within said non-secure storage device for said particular user's private key associated
7	with said certificate;
8	said encryption engine executing code for decrypting said particular user's private key
9	pair; and
10	said encryption engine capable of utilizing said decrypted particular user's private key to
11	encrypt messages transmitted by said application

- 1 --15. (Amended) The system according to claim 14, further comprising said system executing
- code for storing each of said encrypted user private keys in a hard drive.--

B3

- --16. (Amended) The system according to claim 15, further comprising each of said unique user
- key pairs being capable of being utilized only in said data processing system wherein a particular
- user key pair is established, wherein said particular user key pair is not capable of being utilized
- in a second data processing system.--

Please cancel Claim 17.